ip.com PriorArtDatabase

May 13, 2005   USPTO

Search

Full Text

Concept

Document ID

Recent Disclosures

Publish

Publish Disclosure

My IP.com

Manage Account

Prior Purchases

Prior Disclosures

Events

Main Page

Support

Logout

Fingerprint Lookup

Lookup

Displaying records #1 through 10 out of 271

Result # 1   Relevance: ○○○○○

PREVIEW

Public-Key Cryptography Standards (PKCS) #1: RS Cryptography Specifications Version 2.1 (RFC3447

13-Feb-2003   IPCOM000011189D   Englisl

This memo represents a republication of PKCS #1 v2.1 from RS Public-Key Cryptography Standards (PKCS) series, and change retained within the PKCS process. The body of this document is from the PKCS #1 v2.1 document, with certain ...

Result # 2   Relevance: ○○

PREVIEW

PKCS #1: RSA Cryptography Specifications Version (RFC2437)

13-Sep-2000   IPCOM000003015D   Englisl

This memo is the successor to RFC 2313. This document provid recommendations for the implementation of public-key cryptogi the RSA algorithm [18], covering the following aspects:

Result # 3   Relevance: ○○

PREVIEW

PKCS 1: RSA Encryption Version 1.5 (RFC2313)

13-Sep-2000   IPCOM000002879D   Englisl

Status of this Memo

Result # 4   Relevance: ○○

PREVIEW

The TLS Protocol Version 1.0 (RFC2246)

13-Sep-2000   IPCOM000002805D   Englisl

This document specifies Version 1.0 of the Transport Layer Seci protocol. The TLS protocol provides communications privacy ov‹ The protocol allows client/server applications to communicate ir designed to prevent eavesdropping, ...

Result # 5   Relevance: ○○

PREVIEW

RSA/SHA-1 SIGs and RSA KEYs in the Domain Nam (DNS) (RFC3110)

21-Aug-2001   IPCOM000005298D   Englisl

This document describes how to produce RSA/SHA1 SIG resour‹ (RRs) in Section 3 and, so as to completely replace RFC 2537, ‹ to produce RSA KEY RRs in Section 2.

Result # 6   Relevance: ○○

PREVIEW

Privacy Enhancement for Internet Electronic Mail: I Algorithms, Modes, and Identifiers (RFC1423)

12-Sep-2000   IPCOM000002250D   Englisl

This document provides definitions, formats, references, and cit cryptographic algorithms, usage modes, and associated identifi‹ parameters used in support of Privacy Enhanced Mail (PEM) in t community. It is intended to become one member of the ...

Result # 7   Relevance: ⚪⚪⚪⚪⚪

PREVIEW

Look-Ahead Processing for High Speed RSA Crypto Pair Generation

26-Mar-2005   IPCOM000110787D   Englisl

Disclosed is a high performance method for generating cryptogr for the RSA Public Key encryption algorithm.

Result # 8   Relevance: ⚪⚪⚪⚪⚪

PREVIEW

DSA and RSA Key and Signature Encoding for the K Trust Management System (RFC2792)

13-Sep-2000   IPCOM000003391D   Englisl

This memo describes RSA and DSA key and signature encoding, key encoding for version 2 of the KeyNote trust-management s·

Result # 9   Relevance: ⚪⚪⚪⚪⚪

PREVIEW

Algorithms and Identifiers for the Internet X.509 F Infrastructure Certificate and Certificate Revocatio Profile (RFC3279)

10-May-2002   IPCOM000007991D   Englisl

This document specifies algorithm identifiers and ASN.1 encodir digital signatures and subject public keys used in the Internet X Infrastructure (PKI). Digital signatures are used to sign certifica certificate revocation list (CRLs). ...

Result # 10   Relevance: ⚪⚪⚪⚪⚪

PREVIEW

RSA/MD5 KEYs and SIGs in the Domain Name Syst (RFC2537)

13-Sep-2000   IPCOM000003123D   Englisl

A standard method for storing RSA keys and and RSA/MD5 bas· the Domain Name System is described which utilizes DNS KEY ₹ resource records.

Displaying page 1 of 28   < BACK | NEXT >

Search query: RSa

New search | Modify this search | Search within current results

May 13, 2005　　　　　　　　　　USPTO

Search

Full Text

Concept

Document ID

Recent Disclosures

Publish

Publish Disclosure

My IP.com

Manage Account

Prior Purchases

Prior Disclosures

Events

Main Page

Support

Logout

Fingerprint Lookup

Lookup

Displaying records #11 through 20 out of 271

Result # 11　　　Relevance:

PREVIEW

Encryption and Checksum Specifications for Kerbei (RFC3961)

15-Feb-2005　　　　　IPCOM000058124D　　　　　Englisl

This document describes a framework for defining encryption ar mechanisms for use with the Kerberos protocol, defining an abs between the Kerberos protocol and related protocols, and the a mechanisms themselves. The document also defines several ...

Result # 12　　　Relevance:

PREVIEW

Use of the RSAES-OAEP Key Transport Algorithm ir Cryptographic Message Syntax (CMS) (RFC3560)

18-Jul-2003　　　　　IPCOM000016840D　　　　　Englisl

This document describes the conventions for using the RSAES-(transport algorithm with the Cryptographic Message Syntax (CN specifies the enveloped-data content type, which consists of an content and encrypted content-encryption keys for one ...

Result # 13　　　Relevance:

PREVIEW

SEcure Neighbor Discovery (SEND) (RFC3971)

12-Mar-2005　　　　　IPCOM000099093D　　　　　Englisl

IPv6 nodes use the Neighbor Discovery Protocol (NDP) to discov on the link, to determine their link-layer addresses to find route maintain reachability information about the paths to active neig secured, NDP is vulnerable to various ...

Result # 14　　　Relevance:

PREVIEW

Large Virtual Storage Exploitation of Data Space fo

26-Mar-2005　　　　　IPCOM000111160D　　　　　Englisl

This method utilizes large amounts of virtual storage to achieve and fast sorting procedure. Although we present these ideas in the MVS/ESA* Data Space mechanism, our ideas can be extenc areas of virtual storage.

Result # 15　　　Relevance:

PREVIEW

The Secure HyperText Transfer Protocol (RFC2660

13-Sep-2000　　　　　IPCOM000003250D　　　　　Englisl

This memo describes a syntax for securing messages sent usinç Transfer Protocol (HTTP), which forms the basis for the World V Secure HTTP (S-HTTP) provides independently applicable securi transaction confidentiality, ...

Result # 16　　　Relevance:

PREVIEW

Cryptographic Message Syntax (CMS) Algorithms (

05-Sep-2002　　　　　IPCOM000009619D　　　　　Englisl

This document describes the conventions for using several cryp algorithms with the Cryptographic Message Syntax (CMS). The

digitally sign, digest, authenticate, or encrypt arbitrary message

---

Result # 17   Relevance: ⚙

PREVIEW

Application of Identity Keys in the RSA Public Key Cryptosystem

16-Mar-2005   IPCOM000101174D   Englisl

A means is presented for operating the RSA Public Key Cryptos\ single key for enciphering and deciphering the data to be secur(makes use of a special class of keys (called "identity keys"). Op RSA Cryptosystem using a single ...

Result # 18   Relevance: ⚙

PREVIEW

Additional XML Security Uniform Resource Identifii (RFC4051)

13-Apr-2005   IPCOM000124251D   Englisl

A number of Uniform Resource Identifiers (URIs) intended for u Digital Signatures, Encryption, and Canonicalization are defined identify algorithms and types of keying information.

Result # 19   Relevance: ⚙

PREVIEW

Network Specification of Short Length RSA Private

01-Apr-2005   IPCOM000118351D   Englisl

In some networks using RSA cryptography, it may be desirable the length of an RSA private key exponent for performance rea¢

Result # 20   Relevance: ⚙

PREVIEW

The Kerberos Network Authentication Service (V5)

12-Sep-2000   IPCOM000002340D   Englisl

This document gives an overview and specification of Version 5 for the Kerberos network authentication system. Version 4, des elsewhere [1,2], is presently in production use at MIT's Project other Internet sites.

Displaying page 2 of 28   < BACK | NEXT >

Search query: RSa

New search | Modify this search | Search within current results

May 13, 2005   USPTO

Search

- Full Text
- Concept
- Document ID
- Recent Disclosures

Publish

- Publish Disclosure

My IP.com

- Manage Account
- Prior Purchases
- Prior Disclosures
- Events
- Main Page
- Support
- Logout

Fingerprint Lookup

[Lookup]

Displaying records #21 through 30 out of 271

Result # 21   Relevance: ☼☼☼☼☼

PREVIEW

IP Network Address Translator (NAT) Terminology Considerations (RFC2663)

13-Sep-2000   IPCOM000003253D   Englisl

Network Address Translation is a method by which IP addresses from one realm to another, in an attempt to provide transparen hosts. Traditionally, NAT devices are used to connect an isolate with private unregistered addresses to an ...

Result # 22   Relevance: ☼☼☼☼☼

PREVIEW

PKCS 7: Cryptographic Message Syntax Version 1.5

13-Sep-2000   IPCOM000002881D   Englisl

Status of this Memo

Result # 23   Relevance: ☼☼☼☼☼

PREVIEW

Method for RSA Key Agreement

01-Apr-2005   IPCOM000118330D   Englisl

In ANSI X9.42, the Diffie-Hellman key agreement algorithm is t establish a shared secret between communicating parties. After secret is established, it can be used to spawn symmetric algorit DES keys) by concatenating a counter and other public ...

Result # 24   Relevance: ☼☼☼☼☼

PREVIEW

On the Solution of a Certain Congruence Related to Public Key Cryptosystem

22-Mar-2005   IPCOM000108097D   Englisl

In the RSA Public Key Cryptosystem, knowledge by an opponen secretly held phi(m) (sometimes called Euler's totient function), computation of the secretly held decryption key, d. This is accoi using the publicly known encryption key, e, and the ...

Result # 25   Relevance: ☼☼☼☼☼

PREVIEW

The KeyNote Trust-Management System Version 2

13-Sep-2000   IPCOM000003298D   Englisl

This memo describes version 2 of the KeyNote trust-manageme specifies the syntax and semantics of KeyNote `assertions', des attribute' processing, and outlines the application architecture ii KeyNote implementation can be fit. The ...

Result # 26   Relevance: ☼☼☼☼☼

PREVIEW

Internet X.509 Public Key Infrastructure Certificat Profile (RFC2459)

13-Sep-2000   IPCOM000003037D   Englisl

This memo profiles the X.509 v3 certificate and X.509 v2 CRL f(Internet. An overview of the approach and model are provided : introduction. The X.509 v3 certificate format is described in det additional information regarding the format and ...

Result # 27   Relevance: ○ ⟨⟩ ⟨⟩ ⟨⟩

PREVIEW

OpenPGP Message Format (RFC2440)
13-Sep-2000   IPCOM000003018D   Englisl

This document is maintained in order to publish all necessary in
needed to develop interoperable applications based on the Opei
is not a step-by-step cookbook for writing an application. It des
format and methods needed to read, check, ...

Result # 28   Relevance: ○ ⟨⟩ ⟨⟩ ⟨⟩

PREVIEW

DASS - Distributed Authentication Security Service
12-Sep-2000   IPCOM000002336D   Englisl

1.1 What is DASS?

Result # 29   Relevance: ○ ⟨⟩ ⟨⟩ ⟨⟩

PREVIEW

Privacy Enhancement for Internet Electronic Mail: I
Certification and Related Services (RFC1424)
12-Sep-2000   IPCOM000002251D   Englisl

Status of this Memo

Result # 30   Relevance: ○ ⟨⟩ ⟨⟩ ⟨⟩

PREVIEW

Privacy enhancement for Internet electronic mail:
algorithms, modes, and identifiers (RFC1115)
12-Sep-2000   IPCOM000001925D   Englisl

STATUS OF THIS MEMO

Displaying page 3 of 28   < BACK | NEXT >

Search query: RSa

New search | Modify this search | Search within current results

IEEE Xplore

Welcome United States Patent and Trademark Office

Search Results   **BROWSE**   **SEARCH**   **IEEE XPLORE GUIDE**

Results for "((multiple prime)<in>metadata)"   e-mail
Your search matched **1** of **1157693** documents.
A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

» View Session History

» New Search

» Key

IEEE JNL IEEE Journal or Magazine

IEE JNL IEE Journal or Magazine

IEEE CNF IEEE Conference Proceeding

IEE CNF IEE Conference Proceeding

IEEE STD IEEE Standard

Modify Search

((multiple prime)<in>metadata)

☐ Check to search only within this results set

Display Format: ⦿ Citation   ○ Citation & Abstract

☐   **1. Using Prime Numbers for Cache Indexing to Eliminate Conflict Misses**
Kharbutli, M.; Irwin, K.; Yan Solihin; Jaejin Lee;
High Performance Computer Architecture, 2004. HPCA-10. Proceedings. 10th Internation
14-18 Feb. 2004 Page(s):288 - 288

AbstractPlus | Full Text: PDF(600 KB)   **IEEE CNF**

View Selected Items

Help   Contact Us   Privacy & :
© Copyright 2005 IEEE –

Indexed by
Inspec

PORTAL
USPTO

Search: ⊙ The ACM Digital Library   ○ The Guide

multiple primes

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used **multiple** **primes**   Found **45,000** of **154,226**

| Sort results by | relevance ▼ | Save results to a Binder | Try an Advanced Search |
| Display results | expanded form ▼ | Search Tips | Try this search in The ACM Guide |

☐ Open results in a new window

Results 1 - 20 of 200   Result page: **1** 2 3 4 5 6 7 8 9 10   next
Best 200 shown   Relevance scale ☐ ▨ ▨ ▨ ▨

1 Symbolic prime generation for multiple-valued functions
B. Lin, O. Coudert, J. C. Madre
July 1992 **Proceedings of the 29th ACM/IEEE conference on Design automation**

Full text available: 📄 pdf(582.46 KB)   Additional Information: full citation, references, citings, index terms

2 Generating essential primes for a Boolean function with multiple-valued inputs
Y. S. Kuo, W. K. Chou
July 1986 **Proceedings of the 23rd ACM/IEEE conference on Design automation**

Full text available: 📄 pdf(658.92 KB)   Additional Information: full citation, abstract, references, index terms

Detecting essential primes is important in multiple-valued logic minimization. In this paper, We present a fast algorithm that can generate all essential primes without generating a prime cover of the Boolean function. A new consensus operation called asymmetric consensus (acons) is defined. In terms of acons, we prove a necessary and sufficient condition for detecting essential primes for a Boolean function with multiple-valued inputs. The detection of essential primes can be performed by ...

3 The multiple prime random number generator
Alexander Haas
December 1987 **ACM Transactions on Mathematical Software (TOMS)**, Volume 13 Issue 4

Full text available: 📄 pdf(947.78 KB)   Additional Information: full citation, abstract, references, citings, index terms

A new pseudorandom number generator, the Multiple Prime Random Number Generator, has been developed; it is efficient, conceptually simple, flexible, and easy to program. The generator utilizes cycles around prime numbers to guarantee the length of the period, which can easily be programmed to surpass the maximum period of any other presently available random number generator. There are minimum limits placed on the seed values of the variables because the period of the generator is not a fun ...

4 Multiple-output multi-valued prime implicants
William R. Smith, Haresh Shah
May 1976 **Proceedings of the sixth international symposium on Multiple-valued logic**

Full text available: 📄 pdf(233.92 KB)   Additional Information: full citation, abstract, references, index terms

A Generalization of multiple-output techniques to multi-valued functions is introduced for which the prime implicants cover any and all values of the function (value consistent), rather than a single value only (k-cover). The entire set of prime implicants is generated by evaluating a single Petrick-like expansion derived from the truth tables. The work is an extension of a single-output technique developed earlier.

5 Boolean factorization using multiple-valued minimization
Stan Liao, Srinivas Devadas, Abhijit Ghosh
November 1993 **Proceedings of the 1993 IEEE/ACM international conference on Computer-aided design**
Full text available: pdf(657.89 KB)   Additional Information: full citation, references, citings

6 A sublinear additive sieve for finding prime number
Paul Pritchard
January 1981 **Communications of the ACM**, Volume 24 Issue 1
Full text available: pdf(429.51 KB)   Additional Information: full citation, references, citings, index terms

Keywords: algorithms, computational complexity, correctness proofs, prime numbers, sieve

7 Progressive multiple alignment with constraints
Gene Myers, Sanford Selznick, Zheng Zhang, Webb Miller
January 1997 **Proceedings of the first annual international conference on Computational molecular biology**
Full text available: pdf(841.28 KB)   Additional Information: full citation, references, citings, index terms

Keywords: constrained alignment, dynamic programming, multiple sequence alignment

8 Implicit and incremental computation of primes and essential primes of Boolean functions
O. Coudert, J. C. Madre
July 1992 **Proceedings of the 29th ACM/IEEE conference on Design automation**
Full text available: pdf(437.91 KB)   Additional Information: full citation, references, citings, index terms

9 Combination of multiplicative congruential random-number generators with safe prime modulus
Munetaka Sakamoto, Susumu Morito
December 1995 **Proceedings of the 27th conference on Winter simulation**
Full text available: pdf(665.45 KB)   Additional Information: full citation, references, index terms

10 Some new upper bounds on the generation of prime numbers
Harry G. Mairson
September 1977 **Communications of the ACM**, Volume 20 Issue 9

Full text available: pdf(496.87 KB)   Additional Information: full citation, abstract, references, citings

Given an integer N, what is the computational complexity of finding all the primes less than N? A modified sieve of Eratosthenes using doubly linked lists yields an algorithm of OA(N) arithmetic complexity. This upper bound is shown to be equivalent to the theoretical lower bound for sieve methods without preprocessing. Use of preprocessing techniques involving space-time and additive-multiplicative tradeoffs reduces this upper bound to OA(N/log log ...

Keywords: balancing, computational complexity, linked list, number theory, preprocessing, prime number generation, sieve

11 Efficient and portable multiple recursive generators of large order
Lih-Yuan Deng
January 2005 **ACM Transactions on Modeling and Computer Simulation (TOMACS)**, Volume 15 Issue 1
Full text available: pdf(115.99 KB)   Additional Information: full citation, abstract, references, index terms

Deng and Xu [2003] proposed a system of multiple recursive generators of prime modulus p and order k, where all nonzero coefficients of the recurrence are equal. This type of generator is efficient because only a single multiplication is required. It is common to choose $p = 2^{31}-1$ and some multipliers to further improve the speed of the generator. In this case, some fast implementations are available without using explicit division or multiplication. For such ...

Keywords: DX-k generator, GMP, MRG, irreducible polynomial, linear congruential generator, primitive polynomial.

12 The Chinese remainder theorem and the prime memory system
Q. S. Gao
May 1993 **ACM SIGARCH Computer Architecture News , Proceedings of the 20th annual international symposium on Computer architecture**, Volume 21 Issue 2
Full text available: pdf(287.10 KB)   Additional Information: full citation, abstract, references, citings, index terms

As we know, the conflict problem is a very important problem in memory system of super computer, there are two kinds of conflict-free memory system approaches: skewing scheme approach and prime memory system approach. Previously published prime memory approaches are complex or wasting 1/p of the memory space for filling the "holes" [17], where p is the number of memory modules. In this paper, based on Chinese remainder theorem, we present a perfect prime memory system which only ...

13 Recognizing primes in random polynomial time
L. Adleman, M. Huang
January 1987 **Proceedings of the nineteenth annual ACM conference on Theory of computing**
Full text available: pdf(542.84 KB)   Additional Information: full citation, abstract, references, citings, index terms

This paper is the first in a sequence of papers which will prove the existence of a random polynomial time algorithm for the set of primes. The techniques used are from arithmetic algebraic geometry and to a lesser extent algebraic and analytic number theory. The result complements the well known result of Strassen and Soloway that there exists a random polynomial time algorithm for the set of composites.

14 Multiple vs. wide shared bus multiprocessors

A. Hopper, A. Jones, D. Lioupis
April 1989 **ACM SIGARCH Computer Architecture News , Proceedings of the 16th annual international symposium on Computer architecture**, Volume 17 Issue 3

Full text available: pdf(876.64 KB)   Additional Information: full citation, abstract, references, citings, index terms

In this paper we compare the simulated performance of a family of multiprocessor architectures based on a global shared memory. The processors are connected to the memory through caches that snoop one or more shared buses in crossbar arrangement. We have simulated a number of configurations in order to assess the relative performance of multiple versus wide bus machines, with varying amounts of prefetch. Four programs, with widely differing characteristics, were run on each confi ...

15 Symbolic hazard-free minimization and encoding of asynchronous finite state machines

Robert M. Fuhrer, Bill Lin, Steven M. Nowick
December 1995 **Proceedings of the 1995 IEEE/ACM international conference on Computer-aided design**

Full text available: pdf(147.53 KB)   Additional Information: full citation, abstract, references, citings, index terms
Publisher Site

This paper presents an automated method for the synthesis of multiple-input-change (MIC) asynchronous state machines. Asynchronous state machine design is subtle since, unlike synchronous synthesis, logic must be implemented without hazards, and state codes must be chosen carefully to avoid critical races. We formulate and solve an optimal hazard-free and critical race-free encoding problem for a class of MIC asynchronous state machines called burst-mode. Analogous to a paradigm successfully use ...

Keywords: optimal state assignment, asynchronous state machines, hazards, sequential synthesis, sequential optimization

16 A ultra fast Euclidean division algorithm for prime memory systems

Benôit Dupont de Dinechin
August 1991 **Proceedings of the 1991 ACM/IEEE conference on Supercomputing**

Full text available: pdf(931.53 KB)   Additional Information: full citation, references, citings, index terms

17 Algorithm 357: an efficient prime number generator [A1]

Richard C. Singleton
October 1969 **Communications of the ACM**, Volume 12 Issue 10

Full text available: pdf(674.03 KB)   Additional Information: full citation, references, citings, index terms

Keywords: factoring, number theory, prime numbers

18 Algorithm 356: a prime number generator using the treesort principle [A1]

Richard C. Singleton
October 1969 **Communications of the ACM**, Volume 12 Issue 10

Full text available: pdf(674.03 KB)   Additional Information: full citation, references, citings, index terms

Keywords: number theory, prime numbers, sorting

19 Optimization of combinational logic circuits based on compatible gates
Maurizio Damiani, Jerry Chih-Yuan Yang, Giovanni De Micheli
July 1993 **Proceedings of the 30th international conference on Design automation**

Full text available: pdf(756.85 KB) Additional Information: full citation, references, citings, index terms

20 Some negative results concerning prime number generators
Paul Pritchard
January 1984 **Communications of the ACM**, Volume 27 Issue 1

Full text available: pdf(443.17 KB)   Additional Information: full citation, abstract, references, index terms

Programs attributed to Wirth and Misra for generating the prime numbers up to a specified limit are investigated. It is shown that Wirth's program is incorrect according to three increasingly weak criteria, and a composite number is exhibited that the program accepts as prime. This is the smallest known counterexample, and could not have been found by the usual method of program testing—the program would run for trillions of years on the fastest computer before reaching it! CI ...

Keywords: Chinese remainder theorem, prime numbers, program testing

Results 1 - 20 of 200   Result page: **1** 2 3 4 5 6 7 8 9 10   next

Useful downloads: Adobe Acrobat   QuickTime   Windows Media Player   Real Player

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	955	380/28.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/05/13 19:58
S2	44	380/28.ccls. and ((plurality multiple) with primes)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/05/13 20:11
S3	3	380/259.ccls. and ((plurality multiple) with primes)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/05/13 20:08
S4	163	380/259.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/05/13 20:11
S5	6	713/200.ccls. and ((plurality multiple) with primes)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/05/13 20:12
S6	6	713/201.ccls. and ((plurality multiple) with primes)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/05/13 20:12